ABSTRACT OF THE DISCLOSURE

[0035] A method and apparatus is provided in which a trustable operating system is loaded into a region in memory. A start secure operation (SSO) triggers a join secure operation (JSO) to halt all but one central processing unit (CPU) in a multi-processor computer. The SSO causes the active CPU to load a component of an operating system into a specified region in memory, register the identity of the loaded operating system by recording a cryptographic hash of the contents of the specified region in memory, begin executing at a known entry point in the specified region and trigger the JSO to cause the halted CPUs to do the same.

Express Mail Label No. EL414998242US